

# (12) UK Patent Application (19) GB (11) 2 315 967 (13) A

(43) Date of Printing by UK Office 11.02.1998

(21) Application No. 9725279.5

(22) Date of Filing: 30.05.1996

(30) Priority Data

(31) 9610894

(32) 31.05.1995

(33) GB

(86) International Application Data

PCT/EP96/02337 En 30.05.1996

(87) International Publication Data

WO96/38356 En 06.12.1996

(51) INT CL<sup>6</sup>

H04L 12/26 12/18 12/46 29/14

(52) UK CL (Edition P)

H4P PEUX PPG

(56) Documents Cited by ISA

EP 0643486 A EP 0477448 A US 5343485 A

PATENT ABSTRACTS OF JAPAN Vol. 18, no. 300 and  
JP040081145

(58) Field of Search by ISA

INT CL<sup>6</sup> H04L

(71) Applicant(s)

3Com Ireland

(Incorporated in British West Indies)

P O Box 309, Upland House, Georgetown,  
Grand Cayman, Cayman Islands, British West Indies

(74) Agent and/or Address for Service

A A Thornton & Co  
Northumberland House, 303-306 High Holborn,  
LONDON, WC1V 7LE, United Kingdom

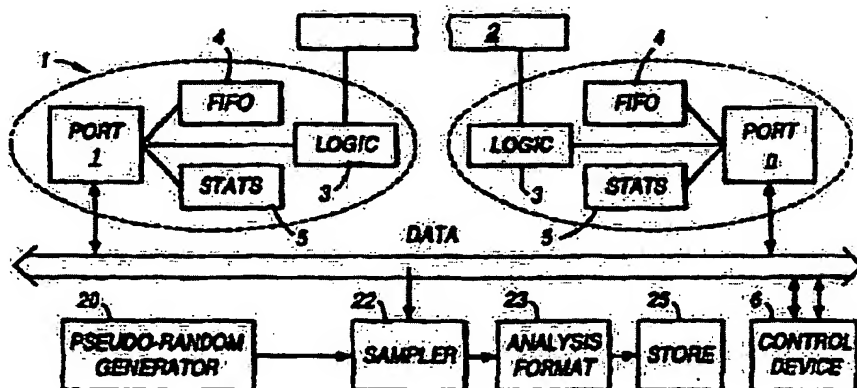
(72) Inventor(s)

Anne O'Connell

Tadhg Creedon

(54) Storm protection mechanism

(57) A method for protecting a network from storms of multicast/broadcast data comprises a switch or bridge which monitors traffic through it in order to detect the onset of a storm condition from previous receptions of request for multicasts or broadcasts. Each port or bridge or switch has associated with it, one data bit which can be controlled to prevent a storm of multicast/broadcast data being forwarded to all parts of the switch and jamming the system.



GB 2 315 967 A

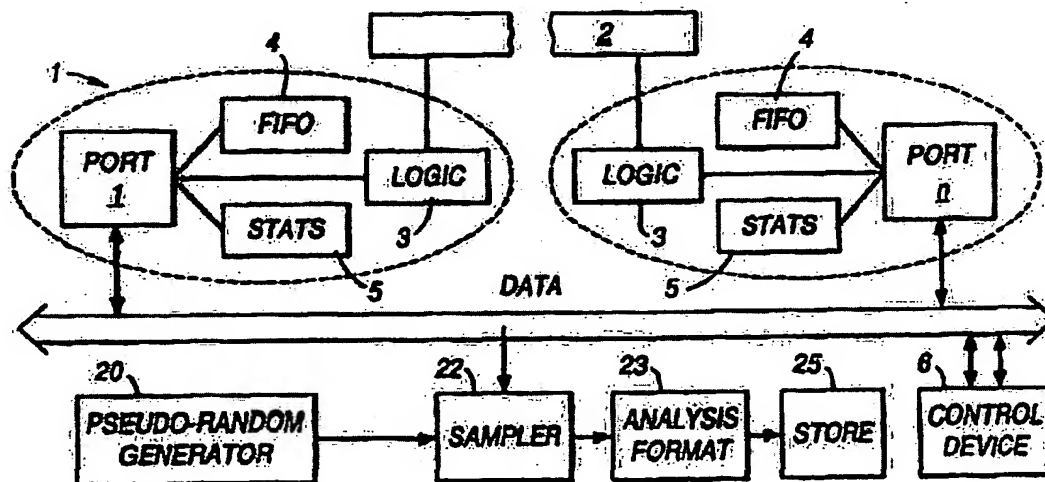




## INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification <sup>6</sup> : H04L 12/26, 12/46, 12/18, 29/14</p>	<p>A1</p>	<p>(11) International Publication Number: WO 96/38956 (43) International Publication Date: 5 December 1996 (05.12.96)</p>
<p>(21) International Application Number: PCT/EP96/02337 (22) International Filing Date: 30 May 1996 (30.05.96) (30) Priority Data: 9510934.4 31 May 1995 (31.05.95) GB (71) Applicant (for all designated States except US): 3COM IRELAND [-/-]; Upland House, P.O. Box 309, Georgetown, Grand Cayman (KY). (72) Inventors; and (73) Inventors/Applicants (for US only): O'CONNELL, Anne [IE/IE]; 3 Woodberry, Carpenterstown Road, Castleknock, Dublin 5 (IE). CREEDON, Tadhg [IE/IE]; Coismeagmore, Furbo, Co. Galway (IE). (74) Agent: CRAWFORD, Andrew, Birkby; A. A. Thornton &amp; Co., Northumberland House, 303-306 High Holborn, London WC1V 7LE (GB).</p>		<p>(81) Designated States: AU, CA, GB, JP, KR, US, European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).  Published With international search report. Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.</p>

(54) Title: STORM PROTECTION MECHANISM



## (57) Abstract

A method for protecting a network from storms of multicast/broadcast data comprises a switch or bridge which monitors traffic through it in order to detect the onset of a storm condition from previous receptions of request for multicasts or broadcasts. Each port or bridge or switch has associated with it, one data bit which can be controlled to prevent a storm of multicast/broadcast data being forwarded to all parts of the switch and jamming the system.

**FOR THE PURPOSES OF INFORMATION ONLY**

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgyzstan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	KZ	Kazakhstan	SG	Singapore
CH	Switzerland	LI	Liechtenstein	SI	Slovenia
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovakia
CM	Cameroon	LR	Liberia	SN	Senegal
CN	China	LT	Lithuania	SZ	Swaziland
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
CZ	Czech Republic	LV	Latvia	TG	Togo
DE	Germany	MC	Monaco	TJ	Tajikistan
DK	Denmark	MD	Republic of Moldova	TT	Trinidad and Tobago
EE	Estonia	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	UG	Uganda
FI	Finland	MN	Mongolia	US	United States of America
FR	France	MR	Mauritania	UZ	Uzbekistan
GA	Gabon			VN	Viet Nam

## STORM PROTECTION MECHANISM

5 The present invention relates to computer network devices and more particularly to bridges or such devices having bridge-like characteristics.

It is customary in computer networks for every device to have a unique address associated with it. Usually networks are designed to allow a one-to-one communication between ports of the network to which the devices are attached, but it is often the case that one port wishes to broadcast the same message to all other ports within the network. While this is acceptable, one has to guard against the possibility of a so-called storm of such broadcast data occurring in view of the fact that this would normally jam buffer stores associated with each port and also with the fact that the whole network would be slowed down.

15 The present invention proposes that a switch or bridge monitors traffic through it, and utilizes certain parameters of the statistics related to the traffic through the bridge or switch in order to detect the onset of a storm condition and takes action to control the level of such traffic within limits.

Preferably, each port has associated with it one bit which can be controlled in order to prevent a storm of multicast/broadcast data being forwarded to all the ports of the switch and jamming the system.

20 The switch or bridge can simply identify from previous receptions of requests for multicasts or broadcasts that it will become overloaded and thus refuse to handle any further request for multicasts or broadcasts until a suitable time.

25 In order that the present invention be more readily understood, an embodiment thereof will now be described by way of example only with reference to the accompanying drawings in which:-

Fig. 1 shows the form of a typical packet of information; and

Fig. 2 shows diagrammatically a circuit layout of a switch or bridge for

explaining the present invention.

As indicated in Fig. 1, a typical packet 10 of information on an ethernet network consists of a block of information 11 indicating the destination address of the packet of information, a source address 12 indicating the device from which the information is derived, other control information 13, actual data 14 to be transmitted, and finally a block 15 indicating any errors which have occurred.

Referring now to Figure 2, a switch or bridge 1 is represented as comprising a number of ports 1...n, only two of which are shown. Data flow through the ports is controlled by a management entity 2 and a control device 6, which allows data transfer between ports. Each port includes a number of circuits including a port logic circuit 3, a data memory 4 for data received by and transmitted by the port and a statistics memory section 5 which stores details of all packets generated by the device (not shown) connected to the port.

In addition to the above, it is also possible to sample data flowing through the bridge or switch. A pseudo random generator 20 is provided which generates a sampling pulse. This sampling pulse operates a gating circuit 22 which feeds information from the next complete packet of a stream of data on the data bus of the network after the timing pulse through an analysis and formatting circuit 23 into the additional memory 25 and then closes the gate at the end of that packet until such time as the next timing pulse is generated by the pseudo random timer.

Either the data from the memory section 5 or data derived from the sampled data can be used for a number of purposes such as the storm protection mechanism which will now be described.

Turning now to the present invention, it is assumed that the networks comprises one or more switches or bridges each having a number of ports as well as a management entity for each switch or bridge. Each of the ports of a switch is known to the management entity of the switch and each port has storage and logic circuits.

In our proposed switch the control device contains a bit associated with each port, which can be altered in response to instructions from the management entity of the switch. The memory section 5 includes stores for logging all traffic through the port including accurate statistics of all broadcast and/or multicast messages created by the device attached to the port.

The management entity monitors traffic through all ports of the switch or bridge and compiles statistics relating to the traffic. Included in the statistics are the number of occasions multicast/broadcast data is being supplied. On the basis of the statistics, from either the total or supplied data or both the management entity makes a decision as to whether to permit a further multicast/broadcast data message to pass through the switch or bridge. If the management entity determines that a storm would result from a further multicast/broadcast data message which would normally jam the memory related with each port and also slow down the network, the management entity then changes the bit associated with the port in the control device 10. The control device on seeing this bit set, will direct any subsequent multicast/broadcast message to a non-existent port of the switch. In our system this is port 31.

It is considered that this system of diversion to a non-existent port is superior to that of simply turning off a port which is attempting to transmit a multicast/broadcast message or of electing all broadcast or multicast traffic input through the port since the statistics relating to usage of the network are being maintained in an accurate form and consequently the management entity can detect when traffic on the network reduces to such a level that further multicast/broadcast message can be accommodated. At that point, the bit per port can be changed back to permit multicast/broadcast messages.

This particular method permits unicast messages to be handled by the network as usual whether or not the storm protection mechanism is in operation.

- 4 -

## CLAIMS:

1. A method for protecting a network from storms whereby analysis is performed on the network traffic, and devices found to be generating large quantities of traffic are prevented from transmitting messages when deemed likely to cause a storm.
2. The method of claim 1 wherein devices are particularly prevented from transmitting multicasts or broadcasts, when a storm is deemed likely.
3. The method of claims 1 or 2 wherein devices which are found to be generating large numbers of multicasts or broadcasts are prevented from transmitting multicasts or broadcasts.
4. The method of any of claims 1 to 3, wherein the analysis is performed on the basis of sampling packets on the network at intervals to generate a stabilised representation of traffic flow.
5. The method of claim 4 wherein the analysis of the network traffic is carried out in real time.
6. The method of either of claims 4 or 5, wherein the sampling is carried out at pseudo random intervals.
7. The method of any of claims 4 to 6, wherein the analysis is performed on whole packets.
8. The method of any of claims 4 to 6, wherein the analysis is performed on particular attributes of the packets.



- 5 -

9. The method of any of claims 4 to 8, wherein further analysis is carried out on the data sampled, which cannot be carried out in real time.

1/1

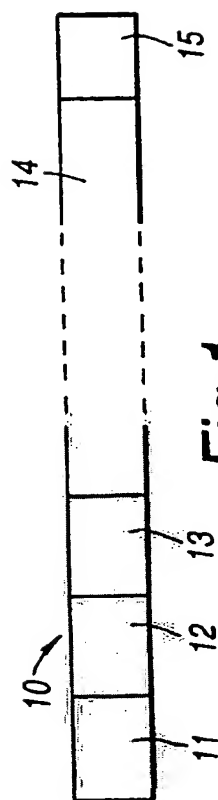


Fig. 1

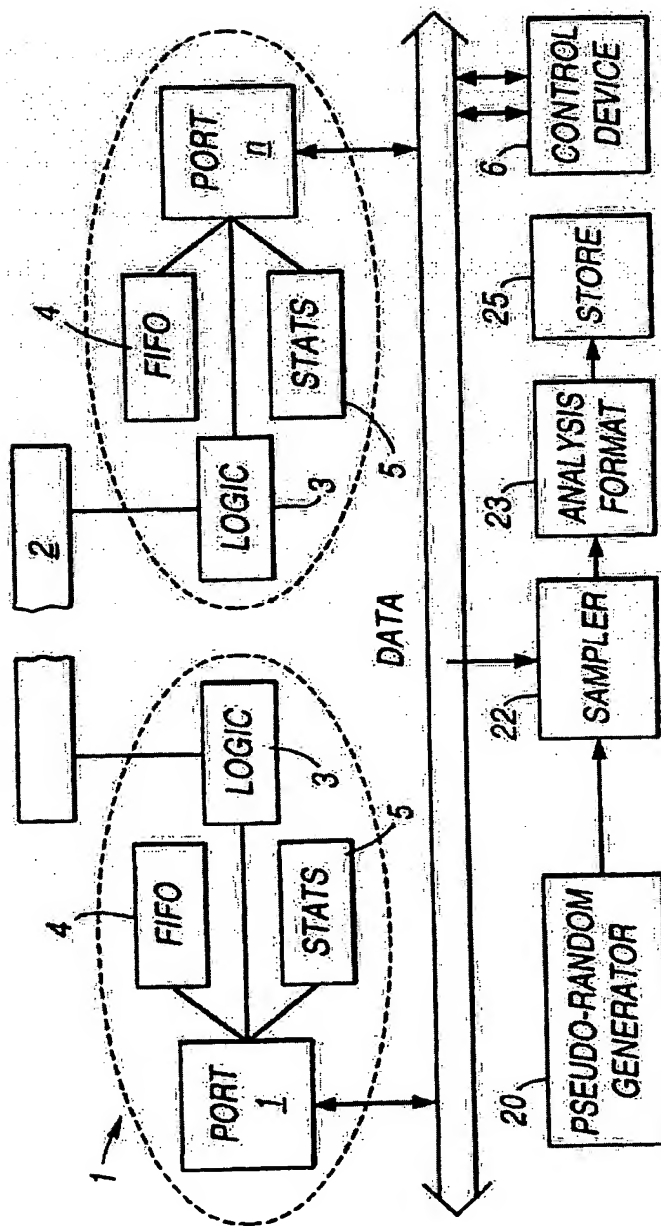


Fig. 2

## INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 96/02337

## A. CLASSIFICATION OF SUBJECT MATTER

IPC 6 H04L12/26 H04L12/46 H04L12/18 H04L29/14

According to International Patent Classification (IPC) or to both national classification and IPC

## B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6 H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

## C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	PATENT ABSTRACTS OF JAPAN vol. 16, no. 300 (E-1227), 2 July 1992 & JP,A,40 081145 (TOSHIBA CORP), 13 March 1992, see abstract	1-3
Y	---	4,6-9
Y	EP,A,0 477 448 (HEWLETT-PACKARD COMPANY) 1 April 1992 see column 1, line 58 - column 2, line 55 see column 4, line 36 - column 5, line 11 see column 7, line 51 - column 8, line 16 ---	4,6-9
A	EP,A,0 542 406 (HEWLETT-PACKARD COMPANY) 19 May 1993 see column 1, line 12 - line 39 see column 1, line 55 - column 2, line 19 see column 3, line 41 - column 4, line 10 ---	1-5,8
	--- -/--	

☒ Further documents are listed in the continuation of box C.☒ Patent family members are listed in annex.

## \* Special categories of cited documents:

- \* "A" document defining the general state of the art which is not considered to be of particular relevance
- \* "E" earlier document but published on or after the international filing date
- \* "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- \* "O" document referring to an oral disclosure, use, exhibition or other means
- \* "P" document published prior to the international filing date but later than the priority date claimed

\* "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

\* "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

\* "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

\* "A" document member of the same patent family

Date of the actual completion of the international search

25 September 1996

Date of mailing of the international search report

04.10.96

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2  
NL - 2280 HV Rijswijk  
Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl,  
Fax: (+ 31-70) 340-3016

Authorized officer

Vaskimo, K

## INTERNATIONAL SEARCH REPORT

International Application No.

PCI/EP 96/02337

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A,5 343 465 (KHALIL) 30 August 1994 see column 2, line 27 - column 3, line 4 see column 4, line 41 - column 5, line 11 see column 12, line 64 - column 13, line 24 -----	4,5

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCI/EP 96/02337

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP-A-477448	01-04-92	CA-A- 2044874	29-03-92
		DE-D- 69020899	17-08-95
		DE-T- 69020899	07-12-95
		EP-A- 0480555	15-04-92
		WO-A- 9206547	16-04-92
		JP-A- 4263536	18-09-92
		JP-T- 5502566	28-04-93
		US-A- 5315500	24-05-94
		US-A- 5450408	12-09-95
EP-A-542406	19-05-93	JP-A- 5260053	08-10-93
US-A-5343465	30-08-94	NONE	

